



Using multi-orbit cyclic subspace codes for constructing optical orthogonal codes

Ferruh Özbudak¹ · Paolo Santonastaso² · Ferdinando Zullo²

Received: 29 May 2024 / Accepted: 11 January 2025 / Published online: 23 January 2025
© The Author(s) 2025

Abstract

We present a new application of multi-orbit cyclic subspace codes to construct large optical orthogonal codes, with the aid of the multiplicative structure of finite fields extensions. This approach is different from earlier approaches using combinatorial and additive (character sum) structures of finite fields. Consequently, we immediately obtain new classes of optical orthogonal codes with different parameters.

Keywords Optical orthogonal code · Cyclic subspace code · Linearized polynomial

Mathematics Subject Classification (2010) 94B60 · 11T30 · 11T71

1 Introduction

In their groundbreaking paper [21], Koetter and Kschischang established the foundations of subspace codes, which turns out to be useful for the error correction in random network coding. Let $\mathbb{F}_q$ be a finite field and $m \geq 2$ be an integer. We consider all $\mathbb{F}_q$ -subspaces of $\mathbb{F}_{q^m}$. If U, V are two $\mathbb{F}_q$ -subspaces of $\mathbb{F}_{q^m}$, then the **subspace distance** $d_s(U, V)$ is defined as

$$d_s(U, V) = \dim_{\mathbb{F}_q}(U) + \dim_{\mathbb{F}_q}(V) - 2 \dim_{\mathbb{F}_q}(U \cap V).$$

In this paper we consider constant dimension $\mathbb{F}_q$ -linear subspaces. Hence let $1 \leq k \leq m$ be a fixed integer. If $\dim_{\mathbb{F}_q}(U) = \dim_{\mathbb{F}_q}(V) = k$, then the subspace distance reads as $d_s(U, V) = 2k - 2 \dim_{\mathbb{F}_q}(U \cap V)$. From now on, let $\mathcal{G}_q(m, k)$ denote the Grassmannian consisting of all k -dimensional $\mathbb{F}_q$ -subspaces of $\mathbb{F}_{q^m}$. There is a natural action of the multiplicative group

✉ Ferdinando Zullo
ferdinando.zullo@unicampania.it

Ferruh Özbudak
ferruh.ozbudak@sabanciuniv.edu

Paolo Santonastaso
paolo.santonastaso@unicampania.it

¹ FENS, Sabancı University, İstanbul, Turkey

² Dipartimento di Matematica e Fisica, Università degli Studi della Campania “Luigi Vanvitelli”, Caserta, Italy

$\mathbb{F}_{q^m}^*$ on $\mathcal{G}_q(m, k)$: for $c \in \mathbb{F}_{q^m}^*$ and $U \in \mathcal{G}_q(m, k)$, let cU denote the action of c on U , which is defined as

$$cU = \{cu : u \in U\} \in \mathcal{G}_q(m, k).$$

Therefore a **cyclic subspace code** C in $\mathcal{G}_q(m, k)$ is a collection of elements of $\mathcal{G}_q(m, k)$ such that $U \in C$ implies $cU \in C$, for every $c \in \mathbb{F}_{q^m}^*$, and $U \in C$ see [17]. It has been an active research area to construct cyclic subspace codes with best parameters in the recent years. One of the most useful techniques in the recent years for the construction of cyclic subspace codes is via Sidon spaces [26]. Here we present an equivalent definition: $U \in \mathcal{G}_q(m, k)$ is a **Sidon space** of dimension k in $\mathbb{F}_{q^m}$ if and only if

$$\dim_{\mathbb{F}_q}(U \cap \alpha U) \leq 1, \text{ for each } \alpha \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q.$$

This suggests a natural extension. For $r \geq 1$, let $U_1, \dots, U_r$ be distinct elements of $\mathcal{G}_q(m, k)$. We say that $\{U_1, \dots, U_r\}$ is an **r -multi Sidon space** if

$$\dim_{\mathbb{F}_q}(U_i \cap \alpha U_j) \leq 1,$$

for every $\alpha \in \mathbb{F}_{q^m}$ and $1 \leq i, j \leq r$ with $i \neq j$, and for every $\alpha \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$ and $i = j$, see [37]. In particular, multi Sidon spaces have important applications in cyclic subspace codes. In this paper, using a multiplicative approach we obtain a new connection between multi-orbit cyclic subspace codes (or equivalently multi Sidon spaces) to optical orthogonal codes.

Given a vector $(x_0, \dots, x_{n-1}) \in \mathbb{F}_2^n$, and for an integer $i \geq n$ we denote by $x_i := x_{i \pmod n}$.

Definition 1.1 An (n, w, λ) **optical orthogonal code (OOC for short)** C is an Hamming-metric code in $\mathbb{F}_2^n$ having constant weight w , satisfying the following two properties:

(1) **The autocorrelation property:**

$$\sum_{t=0}^{n-1} x_t x_{t+\tau} \leq \lambda,$$

for every $(x_0, \dots, x_{n-1}) \in C$ and every integer τ , with $0 < \tau < n$.

(2) **The crosscorrelation property:**

$$\sum_{t=0}^{n-1} x_t y_{t+\tau} \leq \lambda,$$

for every distinct $(x_0, \dots, x_{n-1}), (y_0, \dots, y_{n-1}) \in C$ and every non negative integer τ .

Since every codeword $\mathbf{x} \in C$ has Hamming weight w , the autocorrelation equals w in the extremal case $\tau = 0$. To avoid triviality, we require that $\lambda < w$. For the applications of OOCs in optical code-division multiple access (OCDMA) communication systems, it is desirable that an OOC have large size and small maximum correlation for a given length n and a given weight w ; see [28, 29]. As also pointed out in [13], OOCs when used in OCDMA communication systems need to have the property that each codeword has many more 0's than 1's. In terms of parameters, for an (n, w, λ) OOC, this means that the parameter n is significantly larger than w . However, there is a tradeoff among the parameters of an OOC, known as **Johnson bound**.

Theorem 1.2 (see [20]) *Let C be an (n, w, λ) OOC. Then*

$$|C| \leq J(n, w, \lambda) := \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \frac{n-2}{w-2} \left\lfloor \dots \left\lfloor \frac{n-\lambda}{w-\lambda} \right\rfloor \dots \right\rfloor \right\rfloor \right\rfloor \right\rfloor. \quad (1)$$

When $\lambda = 1$, the optimal set size of an $(n, w, 1)$ OOC is given by

$$|C| = \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \right\rfloor \right\rfloor.$$

There exist several constructions of optimal and large non optimal OOCs with $\lambda = 1$ in the literature, obtained by relying on other areas, such as projective geometry [13, 23], finite field theory [14–16, 31], design theory [1, 8–10, 32, 33] and Sidon sets [27]. Other techniques also involve computer algorithms such as greedy and accelerated greedy algorithms [13] and outer-product matrix algorithm [11].

When $\lambda = 2$, the optimal set size of an $(n, w, 2)$ OOC is given by

$$|C| = \left\lfloor \frac{1}{w} \left\lfloor \frac{n-1}{w-1} \left\lfloor \frac{n-2}{w-2} \right\rfloor \right\rfloor \right\rfloor.$$

The first construction of optimal OOC with $\lambda = 2$ are the $(p^{2h} - 1, p^{h+1}, 2)$ OOCs having size $p^h - 2$, where p is any prime and h is a positive integer, derived from projective geometry and constructed in [14]. Moreover, in [6], new constructions of optimal $(n, w, 2)$ OOC, with $w \in \{4, 6\}$ are obtained. These constructions rely on various techniques in finite projective spaces involving hyperovals in projective planes and Singer groups. Other constructions of large OOCs for $\lambda = 2$ can be found in [12, 18]. When $\lambda > 2$, it is believed that the Johnson bound (1) is not achievable. Apart from the constructions found in [7], where the authors have found optimal $(\frac{q^{h+1}-1}{q-1}, \lambda+1, \lambda)$ OOCs satisfying $\gcd(h+1, i) = 1$ for any $1 \leq i \leq \lambda$, there are no other known constructions. Since for applications, it is very interesting to find OOCs with a large size with respect to their parameters, a well-studied problem in the area of OOCs is dedicated to construct codes that are close to being optimal, starting from the notion of asymptotic optimality introduced in [24]. If an (n, w, λ) OOC C having size $A(n, w, \lambda)$ satisfies

$$\lim_{n \rightarrow +\infty} \frac{A(n, w, \lambda)}{J(n, w, \lambda)} = 1,$$

C is referred to as an **asymptotically optimal OOC**. When $\lambda = 1$, there are constructions of asymptotically optimal OOCs, see e.g [24, 27]. For the case $\lambda = 2$, in [23], the authors, by using conics on finite projective planes in the projective geometry $\text{PG}(3, q)$, where q is a prime power, constructed a family of asymptotically optimal $(q^3 + q^2 + q + 1, q + 1, 2)$ OOCs having size $q^3 - q^2 + q$. Other asymptotically optimal constructions when $\lambda = 2$ are derived in [24]. For the parameters of known asymptotically optimal OOCs with $\lambda = 2$, please consult Table 2 of [7]. By using normal rational curves in $\text{PG}(d, q)$, in [2], the authors constructed a family of asymptotically optimal $(\frac{q^{\lambda+2}-1}{q-1}, q + 1, \lambda)$ OOCs, for any choice of $\lambda > 1$ and $q > \lambda$. In [4], by using normal rational curves and Singer groups, the authors constructed asymptotically optimal OOCs generalizing and improving previous constructions of OOCs, for instance those from conics [23] and arcs [2]. Among the various large constructions of OOCs, the authors have constructed a family of asymptotically optimal designs denoted as $(\frac{q^{h+1}-1}{q-1}, q + 1, \lambda)$, where m and λ are integers satisfying $h > \lambda \geq 2$, and q is a prime power such that $q \geq \lambda$ (refer to [4, Theorem 2]). Additional constructions are presented in [3–5, 7, 24, 25].

We summarize in Table 1 the list of the known largest constructions of OOCs having $\lambda > 2$. Different rows of the tables correspond to different parameters (n, w, λ) of the OOCs.

In this paper we will show a construction of OOCs with the aid of multi-orbit cyclic subspace codes or multi-Sidon spaces. Consequently, we construct new classes of optical orthogonal codes. The rest of the paper is organized as follows. We explain first the connection

Table 1 Known largest family of OOCs with $\lambda > 2$

	Parameters	Conditions	References
1)	$(q^2 - 1, q - 2, 3)$	none	[7, Theorem 14]
2)	$\left(\frac{q^5 - 1}{q - 1}, q, 3\right)$	none	[3, Corollary 4.10]
3)	$\left(\frac{q^{k(\lambda+2)} - 1}{q^k - 1}, q - 1, \lambda\right)$	$\lambda > 1$	[5, Theorem 20]
4)	$\left(\frac{q^{(h+1)} - 1}{q - 1}, q + 1, \lambda\right)$	$h > \lambda > 1$ and $q \geq \lambda$	[4, Theorem 3.4]
5)	$(q^h - 1, q - \lambda + 3, \lambda)$	$h > \lambda \geq 3$ and $q \geq \lambda$	[4, Corollary 5.6]
6)	(ph, h, λ)	p prime and $h \mid (p - 1)$	[24, Theorem 1]
7)	$((q - 1)p, (p - \lambda), \lambda)$	$q = p^a$ and $1 \leq \lambda \leq p - \lambda$	[24, Theorem 2]
8)	$(h(q + 1), h, 2\lambda)$	$q = p^a$, p prime, $h \mid (q - 1)$ and $\gcd(h, q + 1) = 1$	[24, Theorem 3]
9)	$\left(\frac{q^{\lambda-1} - 1}{q - 1}, q + 1, \lambda\right)$	$\lambda \geq 4$	[7, Theorems 11 and 12]
10)	$(q^a - 1, q^h, q^{h-1})$	$a > h \geq 1$	[25, Theorem 11]
11)	$(q - 1, f, \lambda)$	$f \mid (q - 1)$ and $\lambda < f$	[15, Theorem 1] *
12)	$(3^{13f} - 1, 81, 3)$	none	[19, Proposition 3] *

(q is a prime power) (Non asymptotically optimal constructions are marked with *)

to multiplicative structures and finite field extensions in Section 2. Furthermore, we present our constructions of new classes of optical orthogonal codes using a connection to cyclic subspace codes and to multi-Sidon spaces in Section 3. Finally, in Section 4 we show infinitely many new parameters for which we are able to construct OOCs.

2 OOC codes from extension fields

In this section we will see how the problem of finding OOCs can be translated in terms of sets of integers and then we use this correspondence to describe OOCs in extension fields. Let us start by observing that it is possible to establish a one-to-one correspondence between elements of $\mathbb{F}_2^n$ and subsets of $\mathbb{Z}_n$ in the following way:

$$\begin{aligned} \theta : \quad \mathbb{F}_2^n &\longrightarrow 2^{\mathbb{Z}_n} \\ \mathbf{x} = (x_0, \dots, x_{n-1}) &\longmapsto \theta(\mathbf{x}) = \{i \in \mathbb{Z}_n : x_i = 1\}, \end{aligned}$$

so θ is the map that associates each element of $\mathbb{F}_2^n$ with its support (with respect to the Hamming metric). Note also that θ is invertible and $\mathbf{w}_H(\mathbf{x}) = |\theta(\mathbf{x})|$, where $\mathbf{w}_H(\mathbf{x})$ denotes the Hamming weight of $\mathbf{x}$. For a non negative integer τ , and a nonempty subset $X \subseteq \mathbb{Z}_n$ we define

$$X + \tau := \{a + \tau : a \in X\} \subseteq \mathbb{Z}_n.$$

The correspondence given by θ allows us to translate the definition of an OOC in terms of subsets of $\mathbb{Z}_n$.

Definition 2.1 An (n, w, λ) **Optical Orthogonal Set** (OOS) $\mathcal{S}$ is a subset of $2^{\mathbb{Z}_n}$ with the property that $|X| = w$ for every $X \in \mathcal{S}$, and such that the following two properties hold:

(1) The autocorrelation property:

$$|X \cap (X + \tau)| \leq \lambda,$$

for every $X \in \mathcal{S}$ and every integer τ , with $0 < \tau < n$.

(2) The crosscorrelation property:

$$|X \cap (Y + \tau)| \leq \lambda,$$

for every distinct $X, Y \in \mathcal{S}$ and every non negative integer τ .

As a consequence of the properties of θ , we have the following correspondence, showing that constructing OOCs is equivalent to construct sets as defined in Definition 2.1 (OOS).

Lemma 2.2 Let C be an (n, w, λ) OOC. Then $\theta(C)$ is an (n, w, λ) OOS. Conversely, let $\mathcal{S}$ be an (n, w, λ) OOS. Then $\theta^{-1}(\mathcal{S})$ is an (n, w, λ) OOC.

In the next sections, we will provide new families of OOCs by showing new constructions of OOSs. To this aim, we show a procedure to construct OOSs, by using subsets of a finite field. Let ω be a primitive element of $\mathbb{F}_{q^m}$. Let W be a nonempty subset of $\mathbb{F}_{q^m}$. Denote by

$$\mathcal{S}(W) := \{i : \omega^i \in W\} \subseteq \mathbb{Z}_N$$

with $N = q^m - 1$. Note that $|\mathcal{S}(W)| = |W^*|$, where $W^* := W \setminus \{0\}$ and that

$$\mathcal{S}(\alpha W) = \mathcal{S}(W) + \tau, \quad (2)$$

if $\alpha = \omega^\tau$.

In the following result we will see how to construct OOSs, using the multiplicative properties of subsets of $\mathbb{F}_{q^m}$.

Theorem 2.3 Let $W_1, \dots, W_t$ be distinct nonempty subsets of $\mathbb{F}_{q^m}^*$ and let $N = q^m - 1$. Define

$$\mathcal{S}(W_1, \dots, W_t) := \{\mathcal{S}(W_i) : i \in \{1, \dots, t\}\} \subseteq 2^{\mathbb{Z}_N}.$$

The set $\mathcal{S}(W_1, \dots, W_t)$ is an $(q^m - 1, w, \lambda)$ OOS if and only if $|W_i^*| = w$ for every i , and

(1) for every $i \in \{1, \dots, t\}$ and every $\alpha \in \mathbb{F}_{q^m} \setminus \{0, 1\}$

$$|W_i \cap \alpha W_i| \leq \lambda;$$

(2) for every $i, j \in \{1, \dots, t\}$ with $i \neq j$ and every $\alpha \in \mathbb{F}_{q^m}^*$

$$|W_i \cap \alpha W_j| \leq \lambda.$$

In particular, $|\mathcal{S}(W_1, \dots, W_t)| = t$.

Proof By Definition 2.1, $\mathcal{S}(W_1, \dots, W_t)$ is an (N, w, λ) if and only if every set of $\mathcal{S}(W_1, \dots, W_t)$ has size w and

- for any $i \in \{1, \dots, t\}$ and for any $\tau \in \{1, \dots, q^m - 2\}$ then $|\mathcal{S}(W_i) \cap (\mathcal{S}(W_i) + \tau)| = |W_i \cap \omega^\tau W_i| \leq \lambda;$
- for any $i, j \in \{1, \dots, t\}$ with $i \neq j$ and for any $\tau \in \{1, \dots, q^m - 2\}$ then $|\mathcal{S}(W_i) \cap (\mathcal{S}(W_j) + \tau)| = |W_i \cap \omega^\tau W_j| \leq \lambda,$

and so this happens if and only if the W_i 's satisfy (1) and (2). $\square$

In the next section we will see that if we choose the W_i 's as the affine spaces associated with the distinct representative of cyclic subspace codes we obtain an OOS.

3 Constructions from cyclic subspace codes

Let C be a subset of $\mathcal{G}_q(m, k)$, we recall that the **minimum subspace distance** of a subspace code C is defined as

$$d_s(C) := \min\{d_s(U, V) : U, V \in C, U \neq V\}.$$

As already seen in the Introduction, a subspace code $C \subseteq \mathcal{G}_q(m, k)$ is said to be **cyclic** if for every $\alpha \in \mathbb{F}_{q^m}^*$ and every $V \in C$ then $\alpha V \in C$. A **one-orbit (cyclic) code** is a subspace code of the form

$$C_U := \{\alpha U : \alpha \in \mathbb{F}_{q^m}^*\} \subseteq \mathcal{G}_q(m, k),$$

where U is an $\mathbb{F}_q$ -subspace of $\mathbb{F}_{q^m}$ such that $\dim_{\mathbb{F}_q}(U) = k$. Sometimes, C_U is also referred as the **orbit** of U . The size of C_U is $(q^m - 1)/(q^t - 1)$, for some t which divides m . The largest size of such a code is $(q^m - 1)/(q - 1)$, and codes attaining this size are called **full-length one-orbit codes**. Full-length orbit codes with distance $2k - 2$, which is the best possible, will be called **optimal full-length one-orbit codes**. These kinds of subspace codes are connected with Sidon spaces. An $\mathbb{F}_q$ -subspace U of $\mathbb{F}_{q^n}$ is called a **Sidon space** if the product of any two elements of U has a unique factorization over U , up to multiplying by some elements in $\mathbb{F}_q$. More precisely, U is a Sidon space if for all nonzero $a, b, c, d \in U$, if $ab = cd$, then

$$\{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\},$$

where if $e \in \mathbb{F}_{q^m}$ then $e\mathbb{F}_q = \{e\lambda : \lambda \in \mathbb{F}_q\}$.

Theorem 3.1 (see [26, Lemma 34]) *Let U be an $\mathbb{F}_q$ -subspace of $\mathbb{F}_{q^m}$ of dimension k . Then C_U is an optimal full-length one-orbit code if and only if U is a Sidon space.*

The above connection can be extended to multi-orbit cyclic subspace codes. Let $U_1, \dots, U_r$ be $\mathbb{F}_q$ -subspaces of dimension k in $\mathbb{F}_{q^m}$ and let

$$C = \bigcup_{i \in \{1, \dots, r\}} C_{U_i} \subseteq \mathcal{G}_q(m, k) \quad (3)$$

with minimum distance $2k - 2$ and of size $r \frac{q^m - 1}{q - 1}$. These codes have the same minimum distance of the codes associated with Sidon spaces but they are larger.

The code C is uniquely defined by the subspaces $U_1, \dots, U_r$ and therefore we give the following two definitions. The set $\{U_1, \dots, U_r\}$ for the cyclic subspace code (3) is said to be a set of **representatives** of C , whereas if also its minimum distance is $2k - 2$ we will call it a **multi-Sidon space**, in connection with the correspondence between cyclic subspace codes with these parameters with one orbit and Sidon spaces.

We will now show how to use cyclic subspace codes to construct OOCs. First we describe the intersection properties of affine spaces associated with the subspaces of a cyclic subspace code. We start by recalling a well-known property of affine spaces.

Lemma 3.2 *Let V be any vector space over a finite field $\mathbb{F}_q$. For any U_1 and U_2 subspaces of V and $a, b \in V$, we have*

$$|(a + U_1) \cap (b + U_2)| \leq |U_1 \cap U_2|.$$

Proof Suppose that $(a + U_1) \cap (b + U_2) \neq \emptyset$ and consider $v \in (a + U_1) \cap (b + U_2)$. There exist $u_1 \in U_1$ and $u_2 \in U_2$ such that $v = a + u_1 = b + u_2$. It follows that $a = v - u_1$ and $b = v - u_2$ and so

$$a + U_1 = v + U_1 \text{ and } b + U_2 = v + U_2.$$

Hence, $(a + U_1) \cap (b + U_2) = (v + U_1) \cap (v + U_2)$, and so $z \in (v + U_1) \cap (v + U_2)$ if and only if there exist $u'_1 \in U_1$ and $u'_2 \in U_2$ such that $z = v + u'_1 = v + u'_2$. This implies that $u'_1 = u'_2$ and so $z \in v + (U_1 \cap U_2)$ and the assertion follows. $\square$

We are now ready to prove the following result.

Proposition 3.3 *Let $C = \cup_{i \in \{1, \dots, r\}} C_{U_i} \subseteq \mathcal{G}_q(m, k)$ be a cyclic subspace code with minimum distance d and with the property that the C_{U_i} 's are r distinct orbits. For every $i \in \{1, \dots, r\}$, let $d_{i,1}, \dots, d_{i,t}$ be pairwise not $\mathbb{F}_q$ -proportional representatives of the nonzero elements of the quotient $\mathbb{F}_{q^m}/U_i$, with $t = (q^{m-k} - 1)/(q - 1)$. Let*

$$\mathcal{A}(U_1, \dots, U_r) = \bigcup_{i=1}^r \{U_i + d_{i,j} : j \in \{1, \dots, t\}\}.$$

Then

$$|\mathcal{A}(U_1, \dots, U_r)| = t \cdot r,$$

and

(1) for every $V \in \mathcal{A}(U_1, \dots, U_r)$ and every $\alpha \in \mathbb{F}_{q^m} \setminus \{0, 1\}$

$$|V \cap \alpha V| \leq q^{k-d/2},$$

(2) for every $V_1, V_2 \in \mathcal{A}(U_1, \dots, U_r)$ with $V_1 \neq V_2$ and every $\alpha \in \mathbb{F}_{q^m}^*$

$$|V_i \cap \alpha V_j| \leq q^{k-d/2}.$$

Proof For any subspace U in C define the set of affine subspaces associated with U

$$\mathcal{A}(U) = \{U + a : a \in \mathbb{F}_{q^m}^*\}.$$

It is easy to see that $|\mathcal{A}(U)| = |\mathcal{A}(U)|/(q - 1)$ and $|\mathcal{A}(U)| = q^{m-k} - 1$. Since for U_i, U_j , with $i \neq j$ we have that $\mathcal{A}(U_i) \cap \mathcal{A}(U_j) = \emptyset$, we get that

$$|\mathcal{A}(U_1, \dots, U_r)| = \sum_{i=1}^r |\mathcal{A}(U_i)| = r \frac{q^{m-k} - 1}{q - 1},$$

that proves the first part of the assertion. For the second part, we prove (1) and (2).

(1) Let $V \in \mathcal{A}(U_1, \dots, U_r)$. So, $V = U_i + d_{i,j}$, for some $i \in \{1, \dots, r\}$ and $j \in \{1, \dots, t\}$. Let $\alpha \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$. By Lemma 3.2, we have

$$|V \cap \alpha V| = |(U_i + d_{i,j}) \cap (\alpha U_i + \alpha d_{i,j})| \leq |U_i \cap \alpha U_i| \leq q^{k-d/2}.$$

Otherwise, if $\alpha \in \mathbb{F}_q \setminus \{0, 1\}$ then $V \cap \alpha V = (U_i + d_{i,j}) \cap (U_i + \alpha d_{i,j}) = \emptyset$. Indeed, if $V \cap \alpha V = (U_i + d_{i,j}) \cap (U_i + \alpha d_{i,j}) \neq \emptyset$, there exists $u, v \in U_i$ such that $u + d_{i,j} = v + \alpha d_{i,j}$, implying that $d_{i,j} \in U_i$, a contradiction to our hypothesis. This proves (1).

(2) Now, let $V_1, V_2 \in \mathcal{A}(U_1, \dots, U_r)$ with $V_1 \neq V_2$. Assume, that $V_1 = U_i + d_{i,j}$ and $V_2 = U_i + d_{i,h}$, with $j \neq h$. If $\alpha \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$ then, by Lemma 3.2 it follows that

$$V_1 \cap \alpha V_2 = (U_i + d_{i,j}) \cap (\alpha U_i + \alpha d_{i,h}) \leq |U_i \cap \alpha U_i| \leq q^{k-d/2}.$$

Otherwise, if $\alpha \in \mathbb{F}_q^*$, then $(U_i + d_{i,j}) \cap (\alpha U_i + \alpha d_{i,h}) = \emptyset$. Indeed, if $(U_i + d_{i,j}) \cap (\alpha U_i + \alpha d_{i,h}) \neq \emptyset$, there exists $u, v \in U_i$ such that $u + d_{i,j} = v + \alpha d_{i,h}$, implying that $d_{i,j}$ and $d_{i,h}$ are $\mathbb{F}_q$ -proportional representative of the elements of the quotient $\mathbb{F}_{q^m}/U_i$, a contradiction

to our hypothesis. Now, suppose that $V_1 = U_i + d_{i,j_1}$ and $V_2 = U_h + d_{i,j_2}$, with $i \neq h$, therefore using again Lemma 3.2 we have

$$|V_1 \cap \alpha V_2| = |(U_i + d_{i,j_1}) \cap (\alpha U_h + \alpha d_{i,j_2})| \leq |U_i \cap \alpha U_h| \leq q^{k-d/2}.$$

This proves (2) and so the assertion. $\square$

As a consequence we immediately obtain the following result, where we show how to construct OOCs from cyclic subspace codes.

Theorem 3.4 *Let $C = \cup_{i \in \{1, \dots, r\}} C_{U_i} \subseteq \mathcal{G}_q(m, k)$ be a cyclic subspace code with minimum distance d and with the property that the C_{U_i} 's are r distinct orbits. Then $\mathcal{S}(\mathcal{A}(U_1, \dots, U_r))$ is an OOS with size $r(q^{m-k} - 1)/(q - 1)$ and parameters $(q^m - 1, q^k, q^{k-d/2})$. In particular, $\theta^{-1}(\mathcal{S}(\mathcal{A}(U_1, \dots, U_r)))$ is an $(q^m - 1, q^k, q^{k-d/2})$ OOC with size $r(q^{m-k} - 1)/(q - 1)$.*

Proof Consider $\mathcal{A}(U_1, \dots, U_r)$ as in Proposition 3.3. Note that for any $V \in \mathcal{A}(U_1, \dots, U_r)$ we have that

$$|\mathcal{S}(V)| = q^k,$$

and

(1) for every $V \in \mathcal{A}(U_1, \dots, U_r)$ and every $\alpha \in \mathbb{F}_{q^m} \setminus \{0, 1\}$

$$|V \cap \alpha V| \leq q^{k-d/2};$$

(2) for every $V_1, V_2 \in \mathcal{A}(U_1, \dots, U_r)$ with $V_1 \neq V_2$ and every $\alpha \in \mathbb{F}_{q^m}^*$

$$|V_1 \cap \alpha V_2| \leq q^{k-d/2},$$

by Proposition 3.3. By Theorem 2.3 we obtain the assertion. $\square$

Remark 3.5 This construction extends the idea in [19, Section 4] of using certain affine subspaces of the kernel of subspace polynomials. Indeed, in our terms, they consider optimal full-length one-orbit codes defined by the kernel of a trinomial subspace polynomial and then they prove a result of the form of Theorem 3.4 for the studied cases. The problem with this approach is that, in general, it is hard to find in which extension suitable trinomials split completely; see e.g. [22, 30].

Therefore, using large cyclic subspace codes we can construct large OOCs. For a multi-orbit cyclic subspace code $C \subseteq \mathcal{G}_q(m, k)$ having minimum distance d , the sphere-packing bound (see [17, Theorem 2]) implies that

$$|C| \leq \frac{\left[\begin{smallmatrix} m \\ k-d/2+1 \end{smallmatrix} \right]_q}{\left[\begin{smallmatrix} k \\ k-d/2+1 \end{smallmatrix} \right]_q},$$

and so the number r of distinct orbits in C satisfies

$$r \leq \frac{|C|}{q^m - 1} \leq \frac{\left[\begin{smallmatrix} m \\ k-d/2+1 \end{smallmatrix} \right]_q}{(q^m - 1) \left[\begin{smallmatrix} k \\ k-d/2+1 \end{smallmatrix} \right]_q},$$

that is asymptotically r is at most $q^{(m-k)(k-d/2+1)-m}$. Therefore, C defines an $(q^m - 1, q^k, q^{k-d/2})$ OOC with size at most

$$\frac{q^{m-k} - 1}{q - 1} \frac{\left[\begin{matrix} m \\ k - d/2 + 1 \end{matrix} \right]_q}{(q^m - 1) \left[\begin{matrix} k \\ k - d/2 + 1 \end{matrix} \right]_q},$$

and hence asymptotically roughly $q^{(m-k)(k-d/2+1)-k}$

By using Theorem 3.4, we get that C defines an $(q^m - 1, q^k, q^{k-d/2})$ OOC with size $r(q^{m-k} - 1)/(q - 1)$. For such parameters, the Johnson bound (1) can be approximated as follows

$$J(q^m - 1, q^k, q^{k-d/2}) \approx \frac{(q^{n-k})^{q^{k-d/2}}}{q^k},$$

which implies that the constructions of OOCs from cyclic subspace codes cannot be either optimal or asymptotically optimal with respect to the Johnson bound.

4 New constructions of OOCs

In this section we will examine explicit constructions of OOCs from explicit constructions of cyclic subspace codes and we will see OOC constructions with parameters different from those in Table 1. We start by describing the examples of [26, 37].

To this aim we need the following notation: let $\mathcal{L}_{k,q}$ denote the $\mathbb{F}_q$ -algebra of q -polynomials (or linearized polynomials), that is polynomials of this form

$$\sum_{i=0}^t a_i x^{q^i} \in \mathbb{F}_{q^k}[x].$$

For a linearized polynomial $f \in \mathcal{L}_{k,q}$ and an element $\xi \in \mathbb{F}_{q^{rk}} \setminus \mathbb{F}_{q^k}$ we denote

$$W_{f,\xi} = \{x + \xi f(x) : x \in \mathbb{F}_{q^k}\} \subseteq \mathbb{F}_{q^{rk}}.$$

The subset $W_{f,\xi}$ turns out to be an $\mathbb{F}_q$ -subspace of $\mathbb{F}_{q^{rk}}$ of dimension k .

Theorem 4.1 (see [26, 37]) *Let s be a positive integer coprime with $k \geq 2$ and $m = 2k$, let $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$ and let $f_i(x) = \mu_i x^{q^s} \in \mathcal{L}_k$ for $i \in \{1, \dots, r\}$ such that $r \leq q - 1$, $N_{q^k/q}(\mu_i) \neq N_{q^k/q}(\mu_j)$ and $N_{q^k/q}(\mu_i \mu_j \xi^{q^k+1}) \neq 1$ for every $i \neq j$. Then*

$$C = \bigcup_{i=1}^r C_{W_{f_i,\xi}}$$

is a cyclic subspace code of size $r \frac{q^m - 1}{q - 1}$ and minimum distance $m - 2$.

In the next corollary, which is from [26, Construction 37 and Lemma 38], the authors show a possible value for the number r of orbits and a possible choice of the μ_i 's.

Corollary 4.2 *For a prime power $q \geq 3$ and a positive integer $k \geq 2$, let w be a primitive element of $\mathbb{F}_{q^k}$ and let s be a positive integer such that $\gcd(s, k) = 1$. Let $b \in \mathbb{F}_{q^k}$ be such*

that the polynomial $p(x) = x^2 + bx + w$ is irreducible over $\mathbb{F}_{q^k}$ and w is not a $(q-1)$ -power in $\mathbb{F}_{q^k}$ (such a b always exist). For $m = 2k$, let $\xi \in \mathbb{F}_{q^m}$ be a root of $p(x)$. For $i \in \{0, 1, \dots, r-1\}$, where $r = \lfloor (q-1)/2 \rfloor$, let $\xi_i = w^i \xi$ and let

$$V_i = W_{x^{q^s}, \xi_i} = \{u + u^{q^s} \xi_i : u \in \mathbb{F}_{q^k}\}.$$

The set

$$G_{m,s} = \bigcup_{i \in \{0, 1, \dots, r-1\}} C_{V_i} \subseteq \mathcal{G}_q(m, k)$$

is a subspace code of size $r \cdot (q^m - 1)/(q - 1)$ and minimum distance $m - 2$.

We can now use the above construction in Theorem 3.4 to construct OOSs and OOCs (cf. Theorem 4.1).

Corollary 4.3 *Let s be a positive integer coprime with $k \geq 2$ and $m = 2k$, let $\xi \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$ and let $f_i(x) = \mu_i x^{q^s} \in \mathcal{L}_k$ for $i \in \{1, \dots, r\}$ such that $r \leq q-1$, $N_{q^k/q}(\mu_i) \neq N_{q^k/q}(\mu_j)$ and $N_{q^k/q}(\mu_i \mu_j \xi^{q^k+1}) \neq 1$ for every $i \neq j$. Then*

$$C = \bigcup_{i=1}^r C_{W_{f_i, \xi}}.$$

Consider now the family

$$\mathcal{A} = \mathcal{A}(W_{f_1, \xi}, \dots, W_{f_r, \xi}).$$

Then $\mathcal{S}(\mathcal{A})$ is an OOS with parameters $(q^m - 1, q^k, q)$ of size $r(q^k - 1)/(q - 1)$ and $\theta^{-1}(\mathcal{S}(\mathcal{A}(U_1, \dots, U_r)))$ is an $(q^{2k} - 1, q^k, q)$ OOC with size $r(q^k - 1)/(q - 1)$.

Choosing ξ and the μ_i 's as in Corollary 4.2, we have an $(q^{2k} - 1, q^k, q)$ OOC with size $\lfloor (q-1)/2 \rfloor (q^k - 1)/(q - 1)$.

We can do a case-by-case analysis on the parameters of the OOCs constructed in the above proposition with those in Table 1 and we can show that the parameters of our constructions are new.

Proposition 4.4 *The parameters of the OOCs constructed in Corollary 4.3 are new.*

We will prove the above proposition in a more general context in a few lines.

We can use the largest known constructions of cyclic subspace codes to construct large OOCs. In Table 2 we resume the known parameters of known cyclic subspace codes. We report the family of cyclic subspace codes having the largest number r of orbits, with respect to their parameters.

Combining Theorem 3.4 and the constructions of cyclic subspace codes in Table 2, we show new examples of OOCs.

Theorem 4.5 *The cyclic subspace codes in Table 2 produce OOCs with parameters as in Table 3.*

The i -th row of Table 2 is obtained by applying Theorem 3.4 to the i -th row of Table 3. We will now show that we obtain infinitely many new parameters.

Proposition 4.6 *The OOCs with parameters as in Table 3 are new for any $k > 2$ and $q \geq 3$.*

Table 2 Table with known parameters of cyclic subspace codes

	Parameters	r	References
1	$m = 2k, q > 2$	$r_1 = \left\lfloor \frac{q-1}{2} \right\rfloor$	[26, Lemma 38]
2	$m = ak, a > 2$	$r_2 = (k-1)(q-1)q^{\frac{(e+1)k-1}{q^k-1}},$ $e = (\lceil \frac{m}{2k} \rceil - 2)$	[34, Theorem 3.3]
3	$m = ak, a > 2$	$r_3 = q^k(q-1)q^{\frac{(e+1)k-1}{q^k-1}},$ $e = (\lceil \frac{m}{2k} \rceil - 2)$	[34, Theorem 3.5]
4	$m \geq 6$ and $k \leq \left\lfloor \frac{m-2}{4} \right\rfloor$	1	[26, Theorem 19]
5	$m \geq \binom{k+1}{2}$	1	[26, Theorem 31]
6	$m = ak'$ with $a > 6$ and $k = 2k'$	1	[35, Theorem 3.1]
7	$m \mid (q-1)$ and $k \leq \left\lfloor \frac{m+1}{4} \right\rfloor$	1	[36, Theorem 3.8]
8	$m = ak(k-1)+1, k-1$ power of p and $a > 1$	1	[30, Theorem 7.8]
9	$m = a(k^2-1), k$ and q power of 2 and $a > 1$	1	[30, Theorem 7.9]

Proof We prove the newness of the parameters of OOCs in Table 3 by comparing them with the ones in Table 1. All the OOCs in Table 3 have parameters of the form $(q^m - 1, q^k, q)$, for some q prime power and $m \geq 2k \geq 6$ positive integers.

- (1) Assume that $(q^m - 1, q^k, q) = (\bar{q}^2 - 1, \bar{q} - 2, 3)$. By the equality of the last two parameters, we get $q = 3$ and $\bar{q} = 3^k + 2$. Then by the equality of the first parameter, we get $3^m - 1 = (2 + 3^k)^2 - 1$ and by reducing modulo 3, we get a contradiction.

Table 3 New constructions (q is a power of a prime number p)

	Parameters	Conditions	Size
1	$(q^{2k} - 1, q^k - 1, q)$	$q > 2$	$r_1 \frac{q^k - 1}{q - 1}$
2	$(q^{ak} - 1, q^k - 1, q)$	$a > 2$	$r_2 \frac{q^{k(a-1)} - 1}{q - 1}$
3	$(q^{ak} - 1, q^k - 1, q)$	$a > 2$	$r_3 \frac{q^{k(a-1)} - 1}{q - 1}$
4	$(q^m - 1, q^k - 1, q)$	$m \geq 6$ and $k \leq \left\lfloor \frac{m-2}{4} \right\rfloor$	$\frac{q^{m-k} - 1}{q - 1}$
5	$(q^m - 1, q^k - 1, q)$	$m \geq \binom{k+1}{2}$	$\frac{q^{m-k} - 1}{q - 1}$
6	$(q^m - 1, q^{2k} - 1, q)$	$m = ak/2$ with $a > 6$	$\frac{q^{m-2k} - 1}{q - 1}$
7	$(q^m - 1, q^k - 1, q)$	$m \mid (q-1)$ and $k \leq \left\lfloor \frac{m+1}{4} \right\rfloor$	$\frac{q^{m-k} - 1}{q - 1}$
8	$(q^m - 1, q^k - 1, q)$	$m = ak(k-1) + 1, k-1$ power of p and $a > 1$	$\frac{q^{m-k} - 1}{q - 1}$
9	$(q^m - 1, q^k - 1, q)$	$m = a(k^2 - 1), k$ and q power of 2 and $a > 1$	$\frac{q^{m-k} - 1}{q - 1}$

- (2) Assume that $(q^m - 1, q^k, q) = \left(\frac{\bar{q}^5 - 1}{\bar{q} - 1}, \bar{q}, 3\right)$. By the equality of the last two parameters, we get $q = 3$ and $\bar{q} = 3^k$. Then by the equality of the first parameter, we get $3^m - 1 = \frac{3^{5k} - 1}{3^k - 1}$. By reducing modulo 3, we get a contradiction.
- (3) Assume that $(q^m - 1, q^k, q) = \left(\frac{\bar{q}^{k'(\lambda+2)} - 1}{\bar{q}^{k'} - 1}, \bar{q} - 1, \lambda\right)$. By the equality of the last two parameters, we get $q = \lambda$ and $\bar{q} = \lambda^k + 1$. Then by the equality of the first parameter, we get $\lambda^m - 1 = \frac{(\lambda^k + 1)^{k'(\lambda+2)} - 1}{(\lambda^k + 1)^{k'} - 1}$. By reducing modulo λ^k , we get $-1 = \lambda + 2 \pmod{\lambda^k}$, a contradiction.
- (4) Assume that $(q^m - 1, q^k, q) = \left(\frac{\bar{q}^{(h+1)} - 1}{\bar{q} - 1}, \bar{q} + 1, \lambda\right)$. Using the same argument of the previous case, we obtain again a contradiction.
- (5) Assume that $(q^m - 1, q^k, q) = (\bar{q}^h - 1, \bar{q} - \lambda + 3, \lambda)$. By the equality of the last two parameters, we get $q = \lambda$ and $\bar{q} = \lambda^k + \lambda + 3$. Then by the equality of the first parameters, we get $\lambda^m - 1 = (\lambda^k + \lambda + 3)^h - 1$. Since $\lambda = q > 2$, by comparing the maximum degree of both side of the previous equation, we get that $h = 2$. A contradiction to the fact that $h > \lambda \geq 3$.
- (6) Assume that $(q^m - 1, q^k, q) = (\bar{p}h, h, \lambda)$. By the equality of the last two parameters, we get $q = \lambda$ and $h = \lambda^k$. Then by the equality of the first parameter, we get $\lambda^m - 1 = \bar{p}\lambda^k$. By reducing modulo λ , we get a contradiction.
- (7) Assume that $(q^m - 1, q^k, q) = ((\bar{q} - 1)p, (p - \lambda), \lambda)$. One can argue as in the previous case.
- (8) Assume that $(q^m - 1, q^k, q) = (h(\bar{q} + 1), h, 2\lambda)$. One can argue as in Case (6).
- (9) Assume that $(q^m - 1, q^k, q) = \left(\frac{\bar{q}^{\lambda-1} - 1}{\bar{q} - 1}, \bar{q} + 1, \lambda\right)$. One can argue as in Case (3).
- (10) Assume that $(q^m - 1, q^k, q) = (\bar{q}^a - 1, \bar{q}^h, \bar{q}^{h-1})$. By the equality of the last two parameters, we get $k = 2$, a contradiction.
- (11) Assume that $(q^m - 1, q^k, q) = (\bar{q} - 1, f, \lambda)$. By the equality of the three parameters, we get $\lambda = q$, $f = q^k$ and $\bar{q} = q^m$. Since $f \mid (\bar{q} - 1)$, we have $q^k \mid (q^m - 1)$, a contradiction.

□

Acknowledgements The research of the last two authors was partially supported by the project COMBINE of the University of Campania “Luigi Vanvitelli” and was partially supported by the INdAM - GNSAGA Project *Tensors over finite fields and their applications*, number E53C23001670001.

Author Contributions We all contribute equally to this paper.

Funding Open access funding provided by Università degli Studi della Campania Luigi Vanvitelli within the CRUI-CARE Agreement.

Data Availability No datasets were generated or analysed during the current study.

Declarations

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is

not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

References

1. Abel, J., Buratti, M.: Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes. *J. Comb. Theory Ser. A* **106**(1), 59–75 (2004)
2. Alderson, T.L.: Optical orthogonal codes and arcs in $PG(d, q)$. *Finite Fields Appl.* **13**(4), 762–768 (2007)
3. Alderson, T.L., Mellinger, K.E.: Constructions of optical orthogonal codes from finite geometry. *SIAM J. Discret. Math.* **21**(3), 785–793 (2007)
4. Alderson, T.L., Mellinger, K.E.: Optical orthogonal codes from singer groups. *Advances in Coding Theory and Cryptography*. World Scientific, pp. 51–69 (2007)
5. Alderson, T.L., Mellinger, K.E.: Classes of optical orthogonal codes from arcs in root subspaces. *Discret. Math.* **308**(7), 1093–1101 (2008)
6. Alderson, T.L., Mellinger, K.E.: Families of optimal OOCs with $\lambda = 2$. *IEEE Trans. Inf. Theory* **54**(8), 3722–3724 (2008)
7. Alderson, T.L., Mellinger, K.E.: Geometric constructions of optimal optical orthogonal codes. *Adv. Math. Commun.* **2**(4), 451–467 (2008)
8. Buratti, M.: A powerful method for constructing difference families and optimal optical orthogonal codes. *Des. Codes Crypt.* **5**(1), 13–25 (1995)
9. Buratti, M.: Cyclic designs with block size 4 and related optimal optical orthogonal codes. *Des. Codes Crypt.* **26**(1), 111–125 (2002)
10. Buratti, M., Pasotti, A.: Further progress on difference families with block size 4 or 5. *Des. Codes Crypt.* **56**, 1–20 (2010)
11. Charmchi, H., Salehi, J.A.: Outer-product matrix representation of optical orthogonal codes. *IEEE Trans. Commun.* **54**(6), 983–989 (2006)
12. Chu, W., Colbourn, C.J.: Optimal $(n, 4, 2)$ -OOC of small orders. *Discret. Math.* **279**(1–3), 163–172 (2004)
13. Chung, F.R.K., Salehi, J.A., Wei, V.K.: Optical orthogonal codes: design, analysis and applications. *IEEE Trans. Inf. Theory* **35**(3), 595–604 (1989)
14. Chung, H., Kumar, P.V.: Optical orthogonal codes-new bounds and an optimal construction. *IEEE Trans. Inf. Theory* **36**(4), 866–873 (1990)
15. Ding, C., Xing, C.: Several classes of $(2m-1, w, 2)$ optical orthogonal codes. *Discret. Appl. Math.* **128**(1), 103–120 (2003)
16. Ding, C., Xing, C.: Cyclotomic optical orthogonal codes of composite lengths. *IEEE Trans. Commun.* **52**(2), 263–268 (2004)
17. Etzion, T., Vardy, A.: Error-correcting codes in projective space. *IEEE Trans. Inf. Theory* **57**(2), 1165–1173 (2011)
18. Feng, T., Chang, Y., Ji, L.: Constructions for strictly cyclic 3-designs and applications to optimal oocs with $\lambda = 2$. *J. Comb. Theory Ser. A* **115**(8), 1527–1551 (2008)
19. İrimağzı, C., Özbudak, F.: On two applications of polynomials $xk-cx-d$ over finite fields and more, pp. 14–32. Springer, International Workshop on the Arithmetic of Finite Fields (2022)
20. Johnson, S.: A new upper bound for error-correcting codes. *IRE Trans. Inf. Theory* **8**(3), 203–207 (1962)
21. Koetter, R., Kschischang, F.R.: Coding for errors and erasures in random network coding. *IEEE Trans. Inf. Theory* **54**(8), 3579–3591 (2008)
22. McGuire, G., Mueller, D.: Some results on linearized trinomials that split completely. *Finite Fields Appl. De Gruyter Proc. Math.* 149–164 (2020)
23. Miyamoto, N., Mizuno, H., Shinohara, S.: Optical orthogonal codes obtained from conics on finite projective planes. *Finite Fields Appl.* **10**(3), 405–411 (2004)
24. Moreno, O., Zhang, Z., Kumar, P.V., Zinoviev, V.A.: New constructions of optimal cyclically permutable constant weight codes. *IEEE Trans. Inf. Theory* **41**(2), 448–455 (1995)
25. Omrani, R., Moreno, O., Kumar, P.V.: Improved johnson bounds for optical orthogonal codes with $\lambda > 1$ and some optimal constructions, *Proceedings. International Symposium on Information Theory, 2005. ISIT 2005*. IEEE, pp. 259–263 (2005)
26. Roth, R.M., Raviv, N., Tamo, I.: Construction of Sidon spaces with applications to coding. *IEEE Trans. Inf. Theory* **64**(6), 4412–4422 (2017)
27. Ruiz, H.M., Delgado, L.M., Trujillo, C.A.: A new construction of optimal optical orthogonal codes from Sidon sets. *IEEE Access* **8**, 100749–100753 (2020)

28. Salehi, J.A.: Code division multiple-access techniques in optical fiber networks. i. fundamental principles. *IEEE Trans. Commun.* **37**(8), 824–833 (1989)
29. Salehi, J.A., Brackett, C.A.: Code division multiple-access techniques in optical fiber networks. ii. systems performance analysis. *IEEE Trans. Commun.* **37**(8), 834–842 (1989)
30. Santonastaso, P., Zullo, F.: Linearized trinomials with maximum kernel. *J. Pure Appl. Algebra* **226**(3), 106842 (2022)
31. Weng, C.-S.: Optical orthogonal codes with nonideal cross correlation. *J. Lightwave Technol.* **19**(12), 1856 (2001)
32. Yang, G.-C.: Some new families of optical orthogonal codes for code-division multiple-access fibre-optic networks. *IEE Proc.-Commun.* **142**(6), 363–368 (1995)
33. Yang, G.-C., Fuja, T.E.: Optical orthogonal codes with unequal auto-and cross-correlation constraints. *IEEE Trans. Inf. Theory* **41**(1), 96–106 (1995)
34. Zhang, H., Tang, C., Cao, X.: Large optimal cyclic subspace codes. *Discret. Math.* **347**(7), 114007 (2024)
35. Zhang, H., Tang, C., Hu, X.: New constructions of Sidon spaces and large cyclic constant dimension codes. *Comput. Appl. Math.* **42**(5), 230 (2023)
36. Zhang, T., Ge, G.: New constructions of Sidon spaces. *J. Algebraic Comb.* 1–14 (2022)
37. Zullo, F.: Multi-orbit cyclic subspace codes and linear sets. *Finite Fields Appl.* **87**, 102153 (2023)

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.